Amendments to the CLAIMS

1   1. (currently amended)   A security device comprising:

2   a memory device comprising:

3   a first memory portion configured to store a device ID; ~~and~~

4   a second memory portion configured to store a device secret; <u>and</u>

5   <u>a third memory portion configured to store a service provider data item;</u>

6   a processor connected to the memory device, the processor configured to read the

7   stored device ID from the first memory portion ~~and~~ the stored device secret from the second

8   memory portion<u>, and the stored service provider data item from the third memory portion,</u> and <u>to</u>

9   perform a nonreversible computation using the stored device ID, the stored device secret<u>, the</u>

10   <u>stored service provider data item,</u> and a challenge as seeds; and

11   a communication circuit connected to the processor, the communication circuit

12   configured to receive the challenge from a host device and to communicate a result of the

13   nonreversible computation performed by the processor.

1   2. (canceled)

1   3. (original)   The security device of claim 2, wherein the memory device further

2   comprises:

3   a fourth memory portion configured to store a counter value that is incremented

4   responsive to the service provider data item being changed;

5   wherein the stored counter value is also used to seed the nonreversible

6   computation.

1   4. (original)   The security device of claim 1, wherein the first memory portion

2   comprises a nonvolatile and unalterable memory device.

1   5. (original)   The security device of claim 4, wherein the second memory portion

2   comprises an unalterable memory portion.

1   6. (cancelled)

1   7. (original)   The security device of claim 1, wherein the security device is incorporated

2   into a smart card.

1   8. (canceled)

1   9. (original)   The security device of claim 1, wherein the security device is incorporated

2   into a host device.

1   10. (original) The security device of claim 1, wherein the nonreversible computation is a

2   SHA-1 computation.

1   11. (original) The security device of claim 10, wherein the processor is configured to

2   perform the SHA-1 computation serially.

1   12. (original) The security device of claim 10, wherein the processor is configured to

2   perform the SHA-1 computation in parallel.

1   13. - 16. (canceled)

1   17. (currently amended)   The method of claim 34 ~~15~~, further comprising the step of:

2   enabling an electronic device responsive to a positive authentication of the

3   roaming device ~~received response~~.

1   18. (currently amended)   The method of claim 34 ~~15~~, further comprising the step of:

2   disabling an electronic device responsive to a failure to authenticate the roaming

3   device ~~the received response~~.

1   19. (currently amended)   A system for device authentication, the system comprising:

2   a coprocessor security device configured to store a service provider data item and

3   a device secret; and

4   a host device connected to the coprocessor security device, the host device

5   configured to communicate with the coprocessor security device and a roaming security device,

6   the roaming security device being configured to store a plurality of different service provider

7   data items such that said roaming security device may communicate with a plurality of different

8   service providers;

9   wherein the roaming security device can be authenticated to thereby enable the

10   host device.

1   20. (original) The system of claim 19, further comprising:

2   a printer, wherein the coprocessor security device is attached to the printer.

1   21. (original) The system of claim 19, further comprising a means for attaching the

2   roaming security device to a printer cartridge.

4

1   22. (original) The system of claim 19, further comprising:

2   a means for attaching the roaming security device to a printer.

1   23. (original) The system of claim 20, wherein the printer cartridge is disabled

2   responsive to the roaming security device being removed from the printer cartridge.

1   24. (currently amended)   A method of device authentication, the method comprising

2   the steps of:

3   receiving, at a roaming device, a challenge from a host device;

4   generating, at the roaming device, a first nonreversible computation result,

5   wherein the first nonreversible computation result is computed by seeding a first nonreversible

6   algorithm with at least the challenge, a selected service provider data item, and a roaming device

7   secret; and

8   outputting to the host device a response to the challenge, wherein the outputted

9   response includes the first nonreversible computation result,

10   outputting to the host an identification and at least another data item including

11   one of a plurality of service provider data items;

12   generating, at the host device a second nonreversible computation result, wherein

13   the second nonreversible computation result is computed by seeding a second nonreversible

14   algorithm with at least a challenge, said selected service provider data item and a host device

15   secret;

16   comparing, by said host device, said first nonreversible computation and said

17   second nonreversible computation in order to authenticate the roaming device.

1   25. - 26. (canceled)

1   27. (currently amended)   The method of claim 24, further comprising ~~the step of~~:

2   enabling an electronic device responsive to a positive authentication of the

3   ~~received response~~ roaming device.

1   28. (currently amended)   The method of claim 24, further comprising ~~the step of~~:

2   disabling an electronic device responsive to a failure to authenticate the roaming

3   device ~~received response~~.

1   29. (currently amended)   The method of claim 24, wherein the first nonreversible

2   computation result is computed by further seeding the first nonreversible algorithm with a

3   unique device identifier.

1   30. - 33. (canceled)

1   34.   (new) A method of device authentication for a plurality of service providers

2   comprising the steps of:

3   receiving, by a roaming device, a challenge from a device;

4   generating, by said roaming device, a first nonreversible computation result;

5   outputting, by said roaming device to said device, a response to the challenge,

6   wherein the outputted response includes the first nonreversible computation result; wherein the

7   first nonreversible computation result is computed by seeding an algorithm with the received

8   challenge, a secret known by said roaming device and said device, a unique roaming device

9   identifier and one of a plurality of service provider identifiers;

10   reading, by said device from said roaming device, at least said unique roaming

11   device identifier;

12   generating, by said device, a second nonreversible computation result, wherein

13   said second nonreversible computational result is computed by seeding a second algorithm with

14   said challenge, said secret known by said roaming device and said device, said one of a plurality

15   of service provider identifiers and said unique roaming device identifier read from said roaming

16   device; and

17   comparing said first nonreversible computational result with said second

18   nonreversible computational result in order to authenticate said roaming device for a selected

19   one of a plurality of service providers.